(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 December 2001 (13.12.2001)

PCT

(10) International Publication Number
WO 01/95072 A2

(51) International Patent Classification⁷: G06F 1/00, H04L 29/06

(21) International Application Number: PCT/SE01/01285

(22) International Filing Date: 7 June 2001 (07.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/588,285 7 June 2000 (07.06.2000) US

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventor: DESROCHERS, Stéphane; 48 de L'Ermitage, Blainville, Quebec J7B 1K3 (CA).

(74) Agent: MAGNUSSON, Monica; Ericsson Radio Systems AB, Patent Unit Radio Access, S-164 80 Stockholm (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/95072 A2

(54) Title: NETWORK AGENT PASSWORD STORAGE AND RETRIEVAL SCHEME

(57) Abstract: A password storage and retrieval system (8) for secure authentication and management of network agents (10). The password storage and retrieval system (8) includes a memory unit (18) and, in a network agent (10), a decryptor (12), an encryptor (14), and an encryption key (16). The decryptor (12) uses a symmetrical algorithm and an encryption key (16) to decrypt an encrypted password related to the network agent (10) to thereby obtain a decrypted password. The same symmetrical algorithm was previously used to encrypt the password with the key and store the encrypted password. In a preferred embodiment of the invention, the encryption key (16) is hard-coded in the network agent (10), and the memory unit (18) for the encrypted password is a designated directory easily accessible to the network agent (10). An obvious advantage of this invention is that in order to break through the system, a person would need to obtain at least two pieces of information; that is, the encryption key (16) and the encrypted password.

Network Agent Password Storage and Retrieval Scheme

FIELD OF THE INVENTION

The present invention relates to a network agent password storage and retrieval scheme. More specifically, the present invention is concerned with a password storage and retrieval system and method, for network agents.

BACKGROUND OF THE INVENTION

Such as with human users, network agents need to use password(s) to be authorised to perform certain routines with other devices or components. For human users, a standard procedure is to use a password that is memorised and stored in a password database in the network. A system or device for which the user requires to use his/her password also uses the password database. The procedure begins with a user giving his password to the system or device, which will then compare the password with the corresponding password stored in the password database. If a match occurs, then the user is authorised.

In a similar manner, in a multi-component network, network agents requiring performing of routines with other network components (also referred to herewith sometimes as authenticating devices) are requested to provide their identification and password to the authenticating device. The network agent therefore needs to store its password (also referred to herewith as an agent-authenticating password) in a memory location of some sort.

One possible memory location implementation is to use a central database that is accessible to all agents, components or devices in the network. This solution is not very practical since any agent, component, or device, whether it is hostile or not, has access to all the network agent passwords. Indeed, a component needing access to the database to obtain a password must be able to obtain it without having to provide its own password. Additionally, the passwords cannot be encrypted since this involves the use of a password for decryption and the network agent does not have one prior to accessing the central database.

Another solution consists in hard-coding the password within the network agent's code. Unfortunately, this solution renders the network agent very inflexible because its password cannot be changed easily. In addition, if the agent's code is stolen, it can be decompiled and the password extrapolated from the decompiled code.

Yet another proposition consists of storing the password in a file located "close" to the network agent to which it belongs. The file can be placed in a special directory such that it is only accessible to the network agent. However, this prior art proposition stores the password as clear text in the file. Hence, the file can easily be stolen and clear password obtained from it.

OBJECTS OF THE INVENTION

An object of the present invention is therefore to overcome the problems of the prior art and, more specifically, to securely provide password storage and retrieval for a network agent.

SUMMARY OF THE INVENTION

More specifically, in accordance with a first aspect of the present invention, there is provided a password storage and retrieval system for a network agent. The password storage and retrieval system has a memory unit in which an encrypted password related to the network agent is stored, an encryption key related to the network agent and a decryptor for decrypting the encrypted password into a decrypted password for the network agent. The decryptor has access to the encryption key and the memory unit, and includes a password-decrypting algorithm compatible with the encryption key. The decryptor decrypts, in relation to the encryption key, the encrypted password using the password- decrypting algorithm.

Advantageously, the password storage and retrieval system further comprises an encryptor for encrypting an agent password into the encrypted password. The encryptor has access to the encryption key and includes a password-encrypting algorithm compatible with the encryption key. The encryptor encrypts, in relation to the encryption key, the agent password into the encrypted password stored in the memory unit using the password-encrypting algorithm.

In accordance with a third aspect of the invention, there is provided a network agent capable of being authenticated by an authenticating device, and to which is associated an encrypted password stored in a memory unit. The network agent comprises an encryption key related to the network agent, and a decryptor of the encrypted password into a decrypted password authenticating the network agent. The decryptor is connected to the encryption key and the memory unit, and includes a password-decrypting algorithm compatible with the encryption key. The decryptor decrypts, in relation to the encryption key, the encrypted password using the password-decrypting algorithm.

Finally, the present invention is concerned with a method for password storage and retrieval for a network agent, the method comprising steps for storing an encryption key related to the network agent, storing an encrypted password related to the network agent in a memory unit, retrieving, from the memory unit, the encrypted password, reading the encryption key, and decrypting, in relation to the encryption key, the encrypted password into a decrypted password for the network agent.

Advantageously, the password storage and retrieval method further comprises encrypting an agent-authenticating password into the encrypted password in relation to the encryption key, and storing the encrypted password in the memory unit.

An obvious advantage of this invention is that in order to break through the system, a person would need to obtain at least two pieces of information; that is, the encryption key and the encrypted password.

Other objects, advantages and features of the present invention will become more apparent upon reading of the following non-restrictive description of a preferred embodiment thereof, given by way of example only with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be better understood and its numerous objects and advantages will become more apparent to those skilled in the art by reference to the following drawings, in conjunction with the accompanying specification, in which, like numerals denote like parts:

Figure 1 is a schematic block diagram of a partial view of a multi-component network including a network agent password storage and retrieval system according to an embodiment of the present invention;

Figure 2 is a flow chart illustrating operation of the password storage and retrieval system of Figure 1; and

Figure 3 is a flow chart illustrating a method for changing the password in the password storage and retrieval system of Figure 1.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Figure 1 of the appended drawings illustrates a preferred embodiment of the network agent password storage and retrieval system 8 according to the present invention.

Referring to Figure 1, a password storage and retrieval system 8 is shown in interaction with a network agent 10. The network agent may consist, without being limited thereto, of a node of a network, of a module of a node of the network, of a procedure or function of one of the modules of the node of the network. As a non-limitative example, the network agent 10 is a network agent performing a predetermined function in the network. The predetermined function may include, in particular but not exclusively, at least one of the following functions: a management function, a control function, a verification function, a signalling function, a monitoring function, etc. Therefore, the network agent 10 includes additional circuitry, or network agent logic 6 for carrying out its function(s) in the network.

Furthermore, for exemplary purposes only, the network agent 10 is shown to be in interaction with an authenticating device 34, which typically requires a password from the network agent 10 to authenticate the network agent. However, the network agent 10 could alternatively be in interaction in any node requiring a password from the network agent 10, other then the authenticating device 34. Also, those of ordinary

skill in the art will understand that the block diagram of Figure 1 may form part of a more elaborate network comprising many other network agents or devices (not shown).

The password storage and retrieval system 8 includes within the network agent 10 itself, a decryptor 12, an encryptor 14 and an encryption key 16. The password storage and retrieval system 8 also includes a memory unit 18 in which is stored an encrypted password 7 associated with the network agent 10.

The decryptor 12 and encryptor 14 use a symmetrical encrypting mechanism, as well known to those skilled in the art. The decryptor 12 and the encryptor 14 have access to the encryption key 16 through a link 20, so that the encryption key 16 related to the network agent 10 is accessible to both the decryptor 12 and the encryptor 14. Preferably, the encryption key 16 is accessible only by the network agent 10 or by its intricate components.

The encryption key 16 is preferably hard-coded, or intertwined within the code of the network agent 10. In an alternate manner, it is also within the scope of the present invention to use any type of memory circuit and/or data memory support suitable for storing the encryption key 16, which will ensure that the encryption key 16 is accessible only by the network agent 10. For example, in another preferred embodiment, the encryption key 16 is stored in a read-only memory (ROM) (not shown).

The memory unit 18 may store the encrypted password for only one network agent, or alternatively, encrypted passwords associated with two or more network agents (not shown) similar to network agent 10 could be stored in memory unit 18. Although being shown on Figure 1 as being independent from the network agent 10, the memory unit 18 could alternatively form part of the network agent 10, be hosted by one or several other network components or nodes (not shown) with which the network agent 10 communicates. Alternatively, a dedicated directory or software file accessible only by the network agent 10 may constitute memory unit 18. Again, it is within the scope of the present invention to use any other type of memory circuit and/or persistent data memory support suitable for storing the encrypted password.

However, in a preferred embodiment of the invention, the memory unit 18 is a software file that stores the encrypted password, along with a network agent-identifying portion (e.g., identification numbers, letters, code, etc.) for the network agent 10.

Still referring to Figure 1, and as previously indicated, for exemplary purposes only, an authentication device 34 is shown. The authentication device 34 is connected to the network agent 10 through bi-directional link 28. The principal functions of the authentication device 34 are to receive authenticating password from the network agent 10 and to compare the obtained response to data with an expected result.

Thus, in accordance with the present invention, a password is encrypted and stored in the memory unit 18. When the network agent 10 performs tasks that require its password, the password storage and retrieval system 8 is used. Its decryptor 12 accesses the memory unit 18 to obtain the encrypted password 7, obtains the encryption key 16 through the link 20, and applies the encryption key 16 to its encryption software (not shown), to decrypt the encrypted password 7 into an unencrypted password that can be used by the network agent.

More precisely, for storing an encrypted password in the memory unit 18 of the network agent 10, the first operation consists of choosing a password 36 and supplying it to the network agent 10, or alternatively to the password storage and retrieval system 8 of the network agent 10. The network agent 10 includes circuits (not shown) to transmit the new password to the encryptor 14. The encryptor 14 includes an algorithm compatible with the encryption key 16. As previously indicated, the algorithm is a symmetrical algorithm. Symmetrical algorithms are well known to those of ordinary skill in the art and, accordingly, will not be further described in the present specification. The encryptor 14 accesses the encryption key 16 through link 20 to encrypt the chosen password 36 in relation to the encryption key 16. Following encryption of the chosen password 36, this encrypted password is transmitted from the encryptor 14 to the memory unit 18 through circuits (not shown) of the network agent 10 , where it is stored in memory unit 18 for later use.

Referring to Figures 1 and 2, when the network agent wishes to authenticate itself to the authenticating device 34 (step 202) or any other device in order to obtain the permission to perform a certain operation, which requires from the network agent 10 its password, the network agent 10 proceeds to retrieve its password (step 204). For doing so, the decryptor 12 obtains the encrypted password 7 related to the network agent 10 from the memory unit 18 through a link 24 (step 204). The decryptor 12 then decrypts the encrypted password in relation to the encryption key 16 using the algorithm (a symmetrical algorithm in the preferred embodiment) previously used by the encryptor 14 to encrypt the password (step 206).

Finally, in steps 208 and 210, the decryptor 12 forwards the decrypted password to the authenticating device 34 through the circuits (not shown) of the network agent 10 and the link 28 and continues its regular operation. As known to those skilled in the art, the authenticating device 34 then compares the password received from the decryptor 12 with an expected result stored therein. When a match exists between the password and the expected result, the network agent 10 is authenticated and permission(s) granted. If no match exists, the network agent is not authenticated.

Referring to Figures 1 and 3, there is shown a method for changing the current encrypted password 7 of the password storage and retrieval system 8. In step 302, the network agent 10 receives the new password 36. The new password 36 is transmitted to the network agent using a secure mechanism like Kerberos so that the password storage and retrieval system 8 may verify that the new password 36 being submitted is from an authorized party. If the party requesting a password change is authorized (step 306) then new password 36 is encrypted with encryptor 14 using the encryption key 16 (step 307). This new encrypted password then replaces the currently encrypted password stored in memory unit 18 (step 310). Of course, those of knowledge in the art will understand that upon password change, the nodes of the network, such as the authentication device 34, will have to be notified of the password change so that it may update its expected result for the network agent 10 with the new password (step

312). Step 312 may be performed by the user, the agent 10 or a tool of the agent (not shown).

Those skilled in the art will appreciate that a particular advantage of the present invention is that, in order to break through the system, one needs to obtain at least two pieces of information: the encryption key 16, and the encrypted password 7 from memory unit 18.

Although the present invention has been described hereinabove by way of a preferred embodiment thereof, this embodiment can be modified at will, within the scope of the appended claims, without departing from the spirit and nature of the subject invention.

WHAT IS CLAIMED IS:

1. A password storage and retrieval system for a network agent comprising:

a) a memory unit in which an encrypted password related to the network agent is stored;

b) an encryption key related to the network agent; and

c) a decryptor for retrieving the encrypted password into a decrypted password for the network agent, said decryptor having access to the encryption key and the memory unit, and including a password-decrypting algorithm compatible with the encryption key, wherein said decryptor decrypts, in relation to said encryption key, the encrypted password using said password decrypting algorithm.

2. A password storage and retrieval system as recited in claim 1, wherein the memory unit is connected to the decryptor through the network agent.

3. A password storage and retrieval system as recited in claim 1, wherein said encryption key and said decryptor are located in said network agent.

4. A password storage and retrieval system as recited in claim 1, wherein said network agent comprises hard-code incorporating said encryption key.

5. A password storage and retrieval system as recited in claim 1, wherein said network agent comprises a read-only memory incorporating said encryption key.

6. A password storage and retrieval system as recited in claim 1, further comprising an encryptor, said encryptor having access to the encryption key and including a password-encrypting algorithm compatible with said encryption key, wherein said encryptor encrypts, in relation to the encryption key, an unencrypted password into the encrypted password stored in the memory unit using said password-encrypting algorithm.

7. A password storage and retrieval system as recited in claim 6, wherein said decryptor and encryptor have access to the encryption key through exclusive dedicated connections thereby restricting access to said encryption key to said decryptor and said encryptor.

8. A password storage and retrieval system as defined in claim 6, wherein the password-encrypting algorithm is a symmetrical algorithm.

9. A password storage and retrieval system as recited in claim 1, wherein the password-decrypting algorithm is a symmetrical algorithm.

10. A password storage and retrieval system as recited in claim 1, wherein a network agent-identifying portion is further stored in said memory unit.

11. A network agent capable of being authenticated by a network authentication device and to which is associated an encrypted password stored in a memory unit, said network agent comprising:

a) means for performing a predetermined function on the network;

b) an encryption key related to the network agent; and

c) a decryptor of the encrypted password into a decrypted password authenticating the network agent, said decryptor having access to the encryption key and the memory unit, and including a password-decrypting algorithm compatible with the encryption key, wherein said decryptor decrypts, in relation to said encryption key, the encrypted password using said password-decrypting algorithm.

12. A network agent as recited in claim 11, wherein the memory unit is connected to the decryptor through the network agent.

13. A network agent as recited in claim 11, wherein said encryption key and said decryptor are located in said network agent.

14. A network agent as recited in claim 13, wherein said network agent comprises hard-code incorporating said encryption key.

15. A network agent as recited in claim 11, connected to said network agent authenticating device responsive to the decrypted password.

16. A network agent as recited in claim 11, further comprising a read-only memory incorporating said encryption key.

17. A network agent as recited in claim 11, further comprising an encryptor of an agent-authenticating password into the encrypted password, said encryptor having access to the encryption key and including a password-encrypting algorithm compatible with said encryption key, wherein said encryptor encrypts, in relation to the encryption key, encrypts the agent-authenticating password into the encrypted password stored in the memory unit using said password-encrypting algorithm.

18. A network agent as recited in claim 17, wherein said decryptor and encryptor have access to the encryption key through exclusive dedicated connections thereby restricting access to said encryption key to said decryptor and said encryptor.

19. A network agent as defined in claim 17, wherein the password-encrypting algorithm is a symmetrical algorithm.

20. A network agent as recited in claim 11, wherein the password-decrypting algorithm is a symmetrical algorithm.

21. A network agent as recited in claim 11, wherein a network agent-identifying

portion is further stored in said memory unit.

22. A method for storing and retrieving a password for a network agent, the method comprising steps of:

a) storing an encryption key related to the network agent;

b) storing an encrypted password related to the network agent in a memory unit;

c) retrieving, from the memory unit, the encrypted password; and

d) decrypting, in relation to the encryption key, the encrypted password into a decrypted password for the network agent.

23. A method as recited in claim 22, wherein said network agent comprises hard-code, said encryption key storing comprising storing the encryption key in the hard-code, and the encryption key retrieving comprising retrieving, from said hard-code, said encryption key.

24. A method as recited in claim 23, wherein said encryption key is used exclusively for said decrypting.

25. A method as recited in claim 22, further comprising encrypting an password into the encrypted password in relation to the encryption key, and storing the encrypted password in the memory unit.

26. A method as recited in claim 25, wherein the password encrypting comprises using a symmetrical algorithm.

27. A method as recited in claim 22, wherein the password decrypting comprises using a symmetrical algorithm.

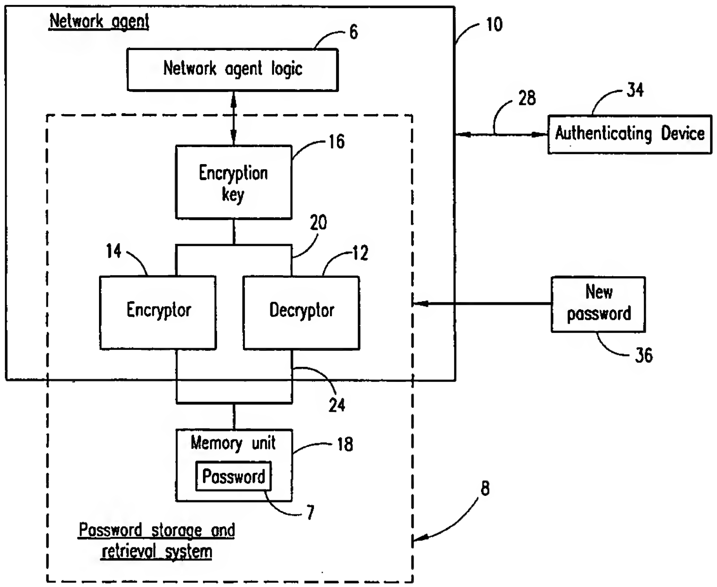


FIG. 1

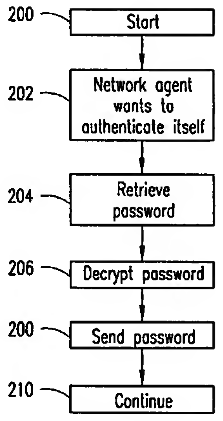

200
Start
202
Network agent wants to authenticate itself
204
Retrieve password
206
Decrypt password
200
Send password
210
Continue

FIG. 2

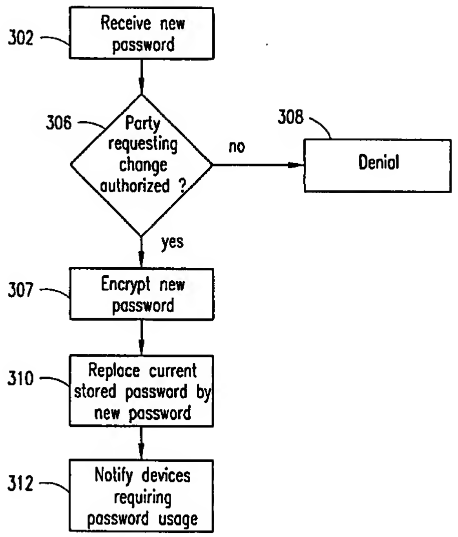

302
Receive new password
306
Party requesting change authorized ?
no
308
Denial
yes
307
Encrypt new password
310
Replace current stored password by new password
312
Notify devices requiring password usage

FIG. 3

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 December 2001 (13.12.2001)

PCT

(10) International Publication Number
WO 01/95072 A3

(51) International Patent Classification⁷: G06F 1/00, H04L 29/06

(21) International Application Number: PCT/SE01/01285

(22) International Filing Date: 7 June 2001 (07.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/588,285 7 June 2000 (07.06.2000) US

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventor: DESROCHERS, Stéphane; 48 de L'Ermitage, Blainville, Quebec J7B 1K3 (CA).

(74) Agent: ERICSSON CANADA INC.; LMC/UP IPR Section, 8400 Decarie Boulevard, Montréal, Québec H4P 2N2 (CA).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

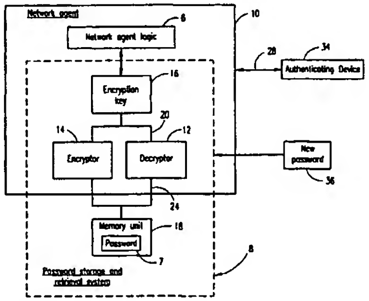
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report: 25 April 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: NETWORK AGENT PASSWORD STORAGE AND RETRIEVAL SCHEME



(57) Abstract: A password storage and retrieval system (8) for secure authentication and management of network agents (10). The password storage and retrieval system (8) includes a memory unit (18) and, in a network agent (10), a decryptor (12), an encryptor (14), and an encryption key (16). The decryptor (12) uses a symmetrical algorithm and an encryption key (16) to decrypt an encrypted password related to the network agent (10) to thereby obtain a decrypted password. The same symmetrical algorithm was previously used to encrypt the password with the key and store the encrypted password. In a preferred embodiment of the invention, the encryption key (16) is hard-coded in the network agent (10), and the memory unit (18) for the encrypted password is a designated directory easily accessible to the network agent (10). An obvious advantage of this invention is that in order to break through the system, a person would need to obtain at least two pieces of information; that is, the encryption key (16) and the encrypted password.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SE 01/01285

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	W FORD ET AL: "Server-assisted generation of a strong secret from a password. In: Enabling technologies: Infrastructure for collaborative enterprises, 2000 (WET ICE 2000)" PROCEEDINGS. IEEE 9TH INTERNATIONAL WORKSHOPS , 14 - 16 June 2000, pages 176-180, XP002902252 the whole document ---	1-27
A	WO 98 45768 A (NORTHERN TELECOM LTD) 15 October 1998 (1998-10-15) the whole document ---	1-27
A	WO 99 13393 A (SECURITY DYNAMICS TECHN) 18 March 1999 (1999-03-18) the whole document ---	1-27
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 17 January 2002	Date of mailing of the international search report 28. 02. 2002
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Marianne Norrgren

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SE 01/01285

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	WO 01 18635 A (SECURE COMPUTING CORP) 15 March 2001 (2001-03-15) the whole document -----	1-27

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/SE 01/01285

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9845768	A	15-10-1998	US	6108420 A	22-08-2000
			AU	6492198 A	30-10-1998
			WO	9845768 A1	15-10-1998
			CN	1255209 T	31-05-2000
			EP	0974084 A1	26-01-2000
WO 9913393	A	18-03-1999	US	6240184 B1	29-05-2001
			AU	9301198 A	29-03-1999
			WO	9913393 A1	18-03-1999
WO 0118635	A	15-03-2001	WO	0118635 A2	15-03-2001